SECURITY AWARENESS NEWSLETTER

Summer 2002

INTRODUCTION

In an effort to emphasize the importance of security issues to all staff and to promote security awareness, the GOT Division of Security Services is pleased to provide this summer security awareness newsletter. It is hoped that the information contained herein will provide practical tips, security solutions, and job-saving techniques.

SECURITY MANUALS AND POLICIES

GOT's Division of Security Services is making an effort to regularly update both GOT internal information systems security policies, as well as enterprise standards and policies. Security manuals and policies are continuously updated. Some of these policies are internal standards for core business security practices within GOT, while other policies apply to agencies outside of GOT and are considered GOT enterprise policies and procedures. GOT staff are encouraged to familiarize themselves with all policies, manuals, and procedures which can be found at GOT Policies and Procedures.

Back to Top

SECURITY TRAINING

In today's world, security is everyone's job. Knowledge of security threats and countermeasures are necessary parts of any administrator's tool kit. The Divisions of Information Technology Training and Security Services are working together to bring SANS Security Essentials class (a lecture style class) on site later this year.

SANS (www.sans.org), the industry leader in security training, offers detailed class that includes lecture and hands-on training on a number of security topics. They even provide services to the FBI and Homeland Office as part of their efforts. The Office of Infrastructure Services (OIS) has a number of staff that are SANS-certified in various areas. More information can be found at http://www.sans.org/onlinetraining/track1.php

Also, the Division of Information Technology Training is trying to confirm other on-site SANS classes in the future. Some of them will be lab and hands-on type classes. More details will follow in future updates.

Anyone who is interested in joining other state agency professionals in the Security Essentials class, please send Frieda Vinson an e-mail expressing your interest or to ask questions.

Back to Top

SECURING INFORMATION IN THE WORKPLACE

In fairy tales, we are often lulled into a sense of comfort and security. The good guys always win and everyone lives happily ever after. In real life, there are no superheroes and the bad guys can ruin happy endings...if we're not careful. The information in our workplace has tremendous value, and if it falls into the wrong hands, the results could be disastrous.

Without realizing it, we often leave confidential data exposed. Unoccupied offices, cluttered desks, unlocked file cabinets and unattended copiers are just a few of the places where sensitive information could be found. Even our trash could be a potential gold mine if it is not disposed of properly.

We may wish for a fairy tale life, but in reality, we must be our own heroes and take an active part in protecting our organization's information. Following the tips below is a fantastic start:

- Secure sensitive files when leaving your work area.
- Do not allow unknown people to "tailgate" into secured areas.
- Do not leave documents unattended on fax machines or photocopiers.

- When finished with conference rooms, wipe boards clean and remove papers.
- Shred confidential documents when discarding them.
- Destroy data diskettes, CDs, and other backup media when discarding them.
- Keep file cabinets and storage rooms containing confidential information locked at all times.
- Alert recipients when sending any confidential information.

Back to Top

ANTI-VIRUS INFORMATION

Klez and its variants continue to lead the malicious code activity. Given its particularly pesky nature, it's not surprising. With its powerful social engineering, address spoofing, and network-spreading capacity, it is becoming the king of all viruses, in terms of its prolificacy. It is even surpassing SirCam, BadTrans, and LoveLetter. Putting a halt to the spread of Klez can be as simple as keeping anti-virus software updated, following safe computing practices, and adhering to the following anti-virus tips posted by McAfee:

Anti-Virus Tips:

- Do not open any files attached to an email from an unknown, suspicious or untrustworthy source.
- Do not open any files attached to an email unless you know what it is, even if it appears to come from a dear friend or someone you know. Some viruses can replicate themselves and spread through email. Better be safe than sorry and confirm that they really sent it.
- Do not open any files attached to an email if the subject line is questionable or unexpected. If the need to do so is there, always save the file to your hard drive before doing so.
- Delete chain emails and junk email. Do not forward or reply to any to them. These types of email are considered spam, which is unsolicited, intrusive mail that clogs up the network.
- Do not download any files from strangers.
- Exercise caution when downloading files from the Internet. Ensure that the source is a legitimate and reputable one. Verify that an anti-virus program checks the files on the download site. If you're uncertain, don't download the file at all or download the file to a floppy and test it with your own anti-virus software.
- Be sure that your anti-virus software (at the office and at home) is updated regularly. Over 500 viruses are discovered each month, so you'll want to be protected. These updates should be at the least the products virus signature files. You may also need to update the product's scanning engine as well.
- Back up your files on a regular basis. If a virus destroys your files, at least you can replace them with your back-up copy. You should store your backup copy in a separate location from your work files, one that is preferably not on your computer.
- When in doubt, always err on the side of caution and do not open, download, or execute any files or email attachments. Not executing is the more important of these

caveats. Check with your product vendors for updates which include those for your operating system web browser, and email . One example is the security site section of Microsoft located at <http://www.microsoft.com/security>.

If you are not sure about a potential virus-related situation, please check with your systems administrator.

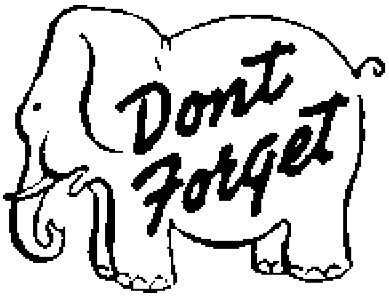
Back to Top

PASSWORDS

If elephants could use computers, they would never write down their passwords. Neither should we. Proper password management is essential to protecting our information.

UserIDs and passwords are uniquely assigned to each of us to grant access and log the activities we perform on our systems. But, if someone else obtains our password, whatever that person does on the system while using it will appear as if we did it. And since we are responsible for every action initiated by our UserID, we need to always protect it from unauthorized access, by locking our workstation every time we leave our area.

Intruders may attempt to gain unauthorized access to our computer systems in various ways. They may look for valid userIDs and passwords that have been written down in the workplace. They may also target computers which are left logged in to our systems. Even software that provides a password-saving feature can compromise our security, as it allows someone to access the system without entering the password.



It doesn't take the memory of an elephant to remember passwords. Keep them confidential by applying the tips below:

- Do not write down or share your passwords.
- Change your passwords regularly.
- Do not allow others to see you enter your passwords.
- Use different passwords on office systems than those you use for personal or Internet accounts.
- Log off your computer at the end of the day.
- Avoid using password-saving features.
- If you leave your computer, always log off. Also, use a password-protected screen saver.
- If you think your password has been compromised, change it immediately and complete a security incident form (GOT-F012), which can be found at http://www.state.ky.us/got/ois/security/Security_forms.htm

Back to Top

GARTNER INFORMATION SECURITY CONFERENCE

GOT and agency staff recently attended Gartner's Information Security Conference, and the following key issues were discussed:

- The InfoSec Scenario: Protecting Enterprise Assets in the New World.
- Competitive Intelligence, Ethics, and the Search for Binladen.
- World Without Secrets: Business, Crime, and Privacy in the Age of Ubiquitous Computing.
- Best Practices in Business Continuity Planning and Disaster Recovery.
- Security at the Speed of E-Business - Managing Security in Times of Rapid Change.
- Human Security Issues: Managing People and Defending Against Social Engineering.
- Creating the Security Aware Enterprise.
- Grant Unified Theory of Information Security.
- Advanced Technology in Information Security: From Smart Cards to Biometrics to Quantum Cryptography.
- The Homeland Security Scenario.
- Protecting Desktops, Laps, and PDA Data.
- Cyber Attacks and Cyber Incident Response Teams.
- Global Aftershocks: Implications for the Resilient Virtual Organization.
- The Secret Service Electronic Crimes Task Force and You - Agency/Enterprise Cooperation.

Back to Top

HACKERS ARRESTED

Ehud Tenebaum, the Israeli man (also known as The Analyzer) who as a teenager broke into computers at MIT, NASA, FBI and the US Department of Defense DoD, received an 18-month jail sentence for his intrusions. Tenebaum initially received a year's probation, a fine and six months of community service, but an appeals court overruled the earlier ruling.

He changed files by unleashing computer viruses, and then deleting files that pointed to his guilt. No dollar estimates were given for the damage. Tenebaum was a partner at a data security startup called 2XS when he was recently sentenced.

Also, Chinese police recently arrested a Taiwanese hacker for breaking into a competitor's computer system and copying the latest programs for its popular online games, according to a report in the Taipei Times. He later posted them on a Web site and allowed players to download them for a fee. "Huang" was allegedly paid NT$20,000 (New Taiwan dollars) by Guangdong's ChuangYu Internet Computerplan Ltd. to steal from Taipei's M-etal Multimedia Co. According to the Criminal Investigation Bureau of the National Police Administration, this is the first reported case of a Chinese firm hiring a Taiwanese hacker to conduct such a cybercrime.

Back to Top

SECURITY CONSIDERATIONS IN WIRELESS NETWORKS

Wireless networks are inherently less secure than a wired network. Security risks inherent in wireless networks are frequently overlooked due to wireless technology's affordability and convenience, which can invite unauthorized access to internal networks and computer systems, as well as the compromise of confidential information.

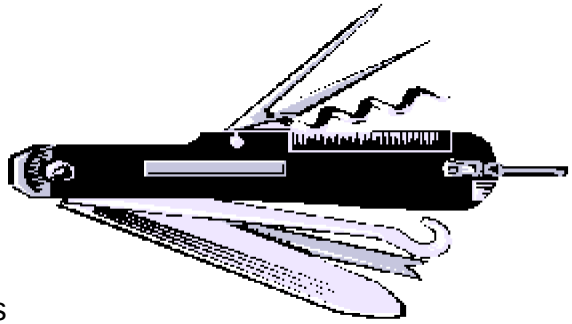
The network traffic on a wireless network is being broadcast like a radio station to the general building location, including the parking lot and roads near the building. Even if the wireless network data and access is not considered important, or is considered public data by the owner, the existence of an unsecured wireless network anywhere in the Kentucky Information Highway (KIH) is an open, unsecured back door for entry into the Commonwealth's critical systems. For these reasons, security must be a primary design criterion BEFORE implementing any wireless network. Wireless technology should be implemented after doing proper due diligence and taking the following appropriate steps to mitigate potential security risks:

- If a wireless network was installed using the manufacturer default settings, GOT recommends that the Access Point(s) (AP) be powered off until security issues can be properly addressed.
- Wireless Networks should be installed using a separate LAN segment, and not installed on existing server or workstation LAN segments. Wireless networks have unique security requirements that are best implemented on LANs separate from other wired devices.
- Carefully control the installation and configuration of Access Points. The installation of an unknown and uncontrolled AP is a wide-open back door to the entire KIH network and should be prohibited.
- Whenever possible or practical, MAC addresses of known devices allowed on the segment should be coded into the Access Point and/or the router to prohibit any unknown devices from using the wireless network for access to the KIH.
- NEVER install a wireless network using the default choices by the wireless manufacturer. This configuration is easy for any hacker to infiltrate.
- If the wireless manufacturer allows changing the Access Point Administrator name, change it. Also, install a strong password for the administrative functions on the wireless LAN on every AP.
- Don't accept the default SSID/ Network ID. Create a unique ID for the networks. You may also want to change the channel from the default. All clients accessing the network must have this same configuration information.
- Use Wired Equivalent Privacy (WEP) to provide encryption between the wireless clients and the Access Point. It is recommended to use at least 128 bit encryption algorithm or stronger whenever possible. Disable SNMP updates to WEP keys if available.
- Secure the AP in a secured location to prevent unauthorized access to the configuration information it stores. If SNMP management is used, change the

community string from the default string“public” to another string. Uses strong passwords wherever possible, and configure the AP to restrict reconfiguration to selected devices, if possible.
- Personal firewalls should be installed on all clients using wireless networks.
- Users should be educated on the effects of running certain services on clients connected to wireless networks, such as remote control software, FTP servers, and shared drives.
- Firewalls, router filters, or other controls should be employed to limit the traffic from wireless networks to only the types of traffic that is expected and only from known clients.
- Consideration should be given to using a Virtual Private Network (VPN) to tunnel the wireless network traffic across any secured networks to a controlled location where proper firewall and security controls can be implemented. This tunnel will protect the secured networks.
- Consideration should be given to using VPN on the wireless clients to further encrypt the network traffic, asWEP is not as secure.
- Consideration should be given to implementing strong authentication for access to the network.
- Servers and other critical devices should never be on the same network as wireless devices.

Back to Top

__ *THE INTERNET - A VERSATILE TOOL*



Like this Swiss Army Knife, the Internet can be remarkably versatile. It can be used to perform a wide range of business functions. In fact, e-commerce is making the Internet a necessity for many organizations.

The Internet is also a popular medium for the exchange of ideas and images. However, some of this material may be considered offensive and does not belong in the workplace. While controversial content may be abundant in cyberspace, we cannot allow it to disrupt the level of professionalism maintained by our organization.

Even though most web sites do not contain offensive material, some may still pose hazards or risks. Web sites can contain "hostile code" that can allow hackers or programs to access our computers. On some sites, viruses may be placed within files that you are encouraged to download. Other Internet functions such as interactive games, chat rooms, and streaming media can consume our valuable system resources.

As you can see, you should be careful when accessing the Internet and follow the guidelines below:

- Limit Internet usage to business-related functions.
- Only download files from reputable web sites.
- Avoid web sites known to contain offensive material.
- Be aware that your Internet surfing can be tracked.
- Do not participate in personal chat rooms.
- Do not use the office Internet connection for game-playing.

Back to Top

MICROSOFT UPDATES

Patch for IIS 4.0 and IIS 5.0 Servers:

There is a new critical exploit to Microsoft IIS 4.0 and IIS 5.0 servers. GOT recommends applying the patch immediately to all IIS installations still using .htr functionality. In the default IIS installation, .htr functionality is enabled. .htr files are used only for web-based password resets. There exists a heap overflow in the server component that is used to handle requests to .htr files.

If the Microsoft IIS Lockdown tool has been used, or htr functionality disabled, there is no need to apply the new patch. If htr functionality is needed for an older application, the patch should be applied immediately. Microsoft rates this as a critical patch for all Internet, Intranet, and Client systems still using .htr, which they recommend disabling if not needed. A new, revised patch issued 7/1/02, and further information is available at the following location: http://www.microsoft.com/ technet/treeview/default.asp?url=/technet/security/bulletin/ms02-028.asp

Cumulative Patch for Windows Media Player:

The Microsoft Security Response Center has released Microsoft Security Bulletin MS02-032 which concerns three newly discovered vulnerabilities in Microsoft Windows Media Player. Customers are advised to review the bulletin and test and deploy the patch in their environment if applicable. More information is now available at http://www.microsoft.com/technet/security/bulletin/MS02-032.asp If you have any questions regarding the patch or its implementation after reading the above listed bulletin you should contact your Systems Administrator.

Cumulative Patches Released for Office, Excel, and Word

Microsoft recently released cumulative patches for a number of Office, Excel and Word vulnerabilities. According to Microsoft, this set of patches will apply all previously released fixes for Excel 2000/2002, Office 200/XP and Word 2002. It will also patch four newly discovered vulnerabilities; two Excel macro execution vulnerabilities, an HTML script execution vulnerability and a new variant of the "Word Mail Merge" vulnerability first addressed in MS00-071. Microsoft recommends applying the patches to affected systems as soon as possible. For more information, see http://www.microsoft.com/technet/security/bulletin/MS02-031.asp

Back to Top

USEFUL URL's

http://www.msn.staysafeonline.com

An easy, kid-friendly guide to the Internet. Beginning with an introduction by TaraLipinski, the program is hosted by Shaquille O' Neal and his animated friends. This simple, 15-minute program helps children (and parents) make smart choices about the use of Internet chat rooms,e-mail, and websites and covers the following:

- Basic rules for communication and online behavior
- The need for online anonymity
- How to protect personal information
- How to identify "Off-Limits" areas for children

http://www.fedcirc.gov/

The Federal Computer Incident Response Center (FedCIRC) is the central coordination and analysis facility dealing with computer security-related issues affecting the civilian agencies and departments of the federal government. FedCIRC's incident response and advisory activities bring together elements of the Department of Defense (DOD), Law Enforcement, Intelligence Community, Academia and computer security specialists from Federal Civilian Agencies and Departments forming a multi-talented virtual security team.

http://www.infosecnews.com/

This on-line news service is backed by SC Magazine - the largest circulation information security magazine. It is read in more than 50 countries around the world and is published in three separate editions in North America, Europe and the Asia Pacific region. The news service gathers information globally through a network of correspondents and over 200 news services. Key links associated with the news direct you to further sources of information relevant to the news item being reported.

http://www.securityfocus.com

SecurityFocus is a leading provider of enterprise security threat management systems. SecurityFocus provides customized and comprehensive alerts of impending cyber attacks worldwide - with countermeasures to prevent attacks before they occur - enabling companies to mitigate risk, manage threats, and ensure business continuity. The company also licenses the world's largest, most complete vulnerability database, hosts the most popular security community mailing list, Bugtraq™, and publishes original security content at www.securityfocus.com.

http://www.computerworld.com/

Computerworld continually provides IT leaders with a host of targeted information services including their award-winning newspaper, web site, email newsletters, events and books. What's more, they provide unmatched reach to IT leaders with targeted advertising and sponsorships.

http://www.terrorism.com/index.shtml

The Terrorism Research Center is dedicated to informing the public of the phenomena of terrorism and information warfare. This site features essays and thought pieces on current issues, as well as links to other terrorism documents, research and resources. Navigate the site by clicking on the area of interest.

http://www.nipc.gov/about/about.htm

Located in the FBI's headquarters building in Washington, D.C., theNIPC brings together representatives from U.S. government agencies, state and local governments, and the private sector in a partnership to protect our nation's critical infrastructures.

Established in February 1998, the NIPC's mission is to serve as the U.S. government's focal point for threat assessment, warning, investigation, and response for threats or attacks against our critical infrastructures. These infrastructures, which include telecommunications, energy, banking and finance, water systems, government operations, and emergency services, are the foundation upon which our industrialized society is based.

Back to Top

***Works Cited**:*

A portion of the material was provided by staffs of Security Wire Digest,SecurityFocus, and Security Awareness, Inc.